Надія Михайлишин
Тернопільський національний економічний університет

ВНУТРІШНІЙ АУДИТ КІБЕРБЕЗПЕКИ КОМПАНІЇ

Активний розвиток цифрових технологій суттєво збільшує обсяги даних, які генеруються компаніями, їх партнерами і клієнтами. Разом з тим, у більшості компаній системи захисту інформації малоефективні проти кіберзлочинців. Тому існує високий ризик злому баз даних і крадіжки важливої інформації.

Міжнародні експерти з кібербезпеки Cybersecurity Ventures підрахували, що в 2019 році кібератаки відбуваються кожні 14 секунд. Із збільшенням кількості кібератак зростає і заподіяний ними збиток. Через хакерські атаки, що спричинили витік даних, у 2018 році компанії втратили $ 3 трлн., а за прогнозом Світового економічного форуму до 2022 року сума планетарного збитку від кібератак може становити $ 8 трлн. [2].

Зростання кількості кібератак змушує компанії забезпечувати свою кібербезпеку, що передбачає захист цифрових даних, інформаційних систем від кібератак.

Основними принципами кібербезпеки є:

– інтеграція кібербезпеки у стратегію компанії;

– захист ключових інформаційних активів;

– виявлення кібератак і ефективне реагування на них з метою мінімізації збитку;

– створення захищеної і стійкої компанії.

Важлива роль у захисті інформації від електронного злому належить внутрішньому аудиту. Кібераудит - це зріз поточного стану кібербезпеки, який дає можливість зрозуміти, де в даний час знаходиться компанія і куди потрібно їй рухатися, щоб стати більш безпечною. За допомогою такого аудиту можна зменшити кіберризики і наслідки їх виникнення.

Виділяють такі види внутрішнього аудиту кібербезпеки компанії:

1. Внутрішній аудит поточних процесів, політик і процедур кібербезпеки. Аудитор досліджує стан реальної безпеки, зокрема з’ясовує, чи проводився тест на проникнення, які його результати, чи виправлені виявлені недоліки; як навчають користувачів з питань кібербезпеки і як оцінюють рівень їх знань; які інциденти, пов’язані з кібербезпекою компанії, були зафіксовані за період, що підлягав аудиту, чи проводилося розслідування і які заходи вживалися для запобігання в майбутньому подібних інцидентів. Такий аудит доцільно проводити після переоцінки поточних ризиків бізнесу.

2. Внутрішній аудит поточного рівня захищеності від кіберзагроз. Включає пошук вразливих місць, моделювання хакерських атак, тести на проникнення і т.п. Цей вид аудиту є перевіркою реагування персоналу на кіберзагрози, а також перевіркою реального впровадження політик, процесів і процедур. Під час перевірки можуть бути виявлені тіньові IT-системи, які формально в компанії не задокументовані і невідомі IT-персоналу.

Робота внутрішніх аудиторів полягає у відстеженні і оцінці ризиків у сфері кібербезпеки. Вони з'ясовують, наскільки сильно бізнес компанії пов'язаний з інформаційними технологіями; які інформаційні системи і ресурси використовуються і наскільки вони критичні; які збитки будуть завдані компанії при порушенні конфіденційності, цілісності і доступності інформації. Зокрема, витік конфіденційної інформації про постачальників, покупців, клієнтів може зумовити їх відтік, або втрату конкурентної переваги; порушення доступності інформації - припинення бізнес-процесу.

Кожен ризик оцінюється за двома параметрами: ймовірністю і потенційним збитком. Виходячи з цих кількісних показників формується карта ризиків і визначається їх пріоритет. Після оцінки кожен кіберризик аналізують і розробляють заходи по роботі з ним. До класичного набору таких заходів належать мінімізація, прийняття, ухилення і диверсифікація. Кіберризики регулярно переоцінюються, а карта кіберризиків, відповідно, переглядається. Такий циклічний підхід допомагає компанії підтримувати максимальний рівень кіберстікості.

Безпосередньо внутрішній аудит кібербезпеки компанії включає декілька етапів:

1. З'ясування кваліфікації внутрішніх аудиторів та достатності ресурсів. Якщо у службі внутрішнього аудиту є співробітники з досвідом роботи у сфері інформаційних технологій або у сфері аудиту інформаційних технологій, то вони після додаткового навчання залучаються до проведення внутрішнього аудиту кібербезпеки. Внутрішні аудитори повинні знати, яка інформація є важливою, як повинні працювати інформаційні системи, що робити у разі виникнення проблеми.

Якщо таких фахівців у компанії немає, то розглядається питання про залучення зовнішніх експертів.

2. Планування і попереднє обстеження. Визначають, які інформаційні системи будуть охоплені внутрішнім аудитом, які сфери будуть вивчатися.

3. Тестування на проникнення. Проводять оцінку безпеки комп'ютерних систем або мереж засобами моделювання атаки зловмисника. Включає сканування, планування атак і проведення атак.

Сканування: збір і аналіз інформації про периметр безпеки; сканування периметру безпеки за допомогою спеціальних інструментів; ідентифікація вразливих зон.

Планування атак: розробка сценаріїв атак на підставі цілей атак і виявлених вразливих зон; підготовка необхідних спеціальних інструментів; оцінка ризиків реалізації атак; планування проведення атак (дата, час).

Проведення атак: проведення атак у запланований час; збір інформації про успішні і неуспішні атаки [3].

Результатом тестування на проникнення є звіт, який включає список виявлених вразливих зон, векторів атаки, досягнутих результатів, рекомендацій щодо їх виправлення.

Література

1. Мусин Э. Аудит кибербезопасности [Электронный ресурс] / Э. Мусин. URL: https://www.audit-it.ru/articles/audit/a105/974194.html
2. Потери организаций от киберпреступности URL: http://www.tadviser.ru/index.php/
3. Уколов А., Богуш Д. Как компании противодействуют киберрискам. IT Risk & Assurance, EY Киев, 27 апреля, 2016. URL: http://mmsa.kpi.ua/sites/default/files/ey-itra-how-companies-face-cyber-risks.pdf

Наталія Мужевич
Тернопільський національний економічний університет

АКТУАЛЬНІ ПИТАННЯ ОБЛІКУ МАЛОЦІННИХ ТА ШВИДКОЗНОШУВАНИХ ПРЕДМЕТІВ

Встановлення ринкової економіки супроводжується удосконаленням бухгалтерського обліку діяльності суб'єктів господарювання. Особливої уваги потребують господарські операції, пов'язані з оборотними активами, які є важливою складовою виробленої готової продукції, визначають собівартість та мають безпосередній вплив на результати діяльності підприємств.

Однією з ділянок обліку, аналізу та контролю в підприємствах усіх форм власності є надходження та витрачання запасів, складовою яких є малоцінні та швидкозношувані предмети (далі – МШП). Даний актив викликає ряд дискусій через те, що МШП (інструменти, прилади, інвентар, канцтовари, спецодяг тощо) відрізняються від інших запасів підприємства, оскільки при їх експлуатації не завжди відбувається їхнє зменшення, як, приміром, із виробничими запасами (сировиною, матеріалами, паливом, запчастинами та ін.), окрім того МШП не